House of Commons Science, Innovation and Technology Select Committee

Call for Evidence – Cyber resilience of the UK's critical national infrastructure

Response by the Institute and Faculty of Actuaries (IFoA)

10 November 2023

The Institute and Faculty of Actuaries (IFoA) is a royal chartered, not-for-profit, professional body. We represent and regulate over 32,000 actuaries worldwide, and oversee their education at all stages of qualification and development throughout their careers. Under our royal charter, we are committed to promoting the public interest as well as developing actuarial science. In order to further these goals, our members participate in a range of practice Boards supported by research working parties. In particular, the Risk Management Board oversees the work of our Cyber Risk Working Party, whose members have expertise in several areas covered by the Committee's Call for Evidence.

Executive summary

1. This response covers the first topic in the Call for Evidence (Part 1) "The types and sources of cyber threats to Critical National Infrastructure (CNI) most critical to the function of the UK digital economy". By industry it focuses on:

    a. Finance – in particular the impact on Insurance – this is covered by our paper on Operational Cyber Risk[i] and also the text on Life Insurance Risk (which does not have an associated paper attached).

    b. The insights from looking at insurance are relevant to all four areas listed in the Call for Evidence (Communications (including space); Energy; Government; and Finance). The paper on Operational Cyber risk is relevant to industries other than insurance, as is the paper on Non-affirmative Cyber Risks/Cyber as a Peril[ii].

2. Part 2 is not covered explicitly but some of our response is relevant. This will chiefly be the read across in respect of public-private partnerships and public entities that will need coverage against Cyber incidents. Similarly Part 4 is also not covered explicitly but our response also covers the requirements for insurance for public private partnerships and certain public entities requiring the insurance as well as the uncertainty in assessing the risk.

3. Parts 3, 5 and 6 have not been covered in this response.

4. The papers linked to at the end of this response were not written as responses to the Select Committee. However, they are very useful to support our comments. There follows a summary of each paper in order to bring out our relevant points in respect of each area. More detail is available in the papers so that the Committee can choose to read further.

Operational Cyber Risk

5. Cyber risk is one of the most important sources of operational risks facing organisations today. The IFoA Cyber Risk Working Party produced a paper helping firms understand the potential impacts of operational risk events as a result of a cyber threat. This summary is largely relevant to insurance.

6. Risk actuaries and other risk management professionals at insurance companies need to have a robust assessment of the potential losses stemming from cyber risk that their organisations may face. They should be able to do this as part of an overall risk management framework and be able to demonstrate this to stakeholders such as regulators and shareholders.

7. The paper describes a proposed framework in which to perform such an assessment by proposing quantification examples of some key scenarios. However, it should be noted that at the time the scenarios focussed predominately on the risk of targeted attacks to the insurance company. The operational risk scenario arising from a failure of critical infrastructure was not considered. More recently financial services generally including insurers have been required to assess their business continuity plans (BCP) which covers the potential for no access for prolonged periods to key IT services such as critical infrastructure.

8. Generally speaking, the insurance market is not critically dependent on access to CNI services over short periods. It is generally considered that short term outages do not have a significant revenue or operating impact. This is largely driven by the nature of the way business is bought by consumers and that insurance products are not considered essential (in most cases). This however is likely to be tested to a greater extent in the personal lines market for products such as life, health, car and travel insurance where short to medium term outages may result in cover not being able to be provided. Again, over a short period the impact is not likely to be significant to either consumers or the industry.

9. Whilst the short-term impact of CNI outages is likely to be a risk that can be managed/absorbed by the industry, longer outages (i.e. multiple weeks to months) would be significant across all areas of the industry. This would undoubtedly affect the following:

    a. Ability of firms to achieve revenue targets

    b. Ability of companies to pay claims in a timely manner

    c. Companies' duty to customers to keep them informed (conduct risks)

    d. Potentially the ability of firms to provide for their own staff (depending on the scale of the CNI).

10. We expect the effects from any long-term outage of CNI services to the insurance industry to be similar to many industries. Whilst COVID-19 was a stark reminder that global systemic events can happen and cause business disruption to many sectors, insurance was much less affected (for the most part) and continued to offer services. Under a major CNI event this may not be the case given increased dependency for the insurance industry on CNI for delivering and conducting its services. Key CNI for insurance would be internet and power to enable remote working and collaboration. However, the fragmented nature of the power and data grids are more likely to result in localised disruption than national disruption and there will be some level of flexibility of some staff to relocate temporarily to areas that are not disrupted. As with Covid, this flexibility will be limited to the extent that staff are parents or carers but a mitigant that increases resilience is the availability of domestic off-grid power and alternative data access methods such as mobile broadband.

11. This risk is further exacerbated by the trend towards a more interconnected, digital and innovative industry. In the pursuit of offering more efficient and valuable services to customers (both corporate and personal lines) insurers are ever expanding their technical

offering e.g. some companies have entirely algorithmic-driven underwriting that depends on the ability for submissions to be made electronically. Combined with the growth of 'Internet of Things;' offerings to enable parametric covers (such as Flood Flash), a major CNI event would render the services either severely limited or all together redundant until brought back online.

12. The worst-case scenario for insurers would be a major CNI event combined with a major catastrophe. This event would restrict the insurer's ability to respond to claim events and deliver the promised services to clients. It would likely require an effort to revert to more traditional paper-based approaches to deal with the crisis. Such an event may be an unprecedented flood at the time of a major CNI event that means policyholders would find it more difficult to claim with insurers and/or communicate with them and vice-versa. This would undoubtably increase the overall cost of the catastrophe to both the insurance industry and public service response.

13. There is currently limited appetite across the industry to deal with digital currencies such as Bitcoin, hence the impact of lack of access to this type of currency would not be a material risk to the industry.

14. Most of the above assumes the CNI event would be an outage to the ability to service clients, but if the CNI event resulted in data breach/leakage of any kind this would result in a unique liability scenario for the courts to resolve. If all policyholder details are leaked due to some access to CNI then the philosophical question of whether any particular company is liable for the usual associated costs would likely be challenged. Typically operational cyber risk events would capture such costs if company failure resulted in the data leak, however if that leak were to arise due to CNI/dependency of shared services the responsibility of the costs becomes less clear.

Non-affirmative Cyber Risks/Cyber as a Peril

15. A company does not necessarily need to be underwriting a cyber policy in order to be exposed to insured losses resulting from a cyber event. The prime examples of this in recent history are business interruption losses where the business interruption was caused by a cyber peril or property damage where the assets were digital assets that were stolen or damaged by cyber events The insurance market has worked hard in recent years to improve policy wordings to ensure that the risk of this is reduced and so that insurers and their clients are both clear on what is and is not covered in respect of cyber.

16. Nonetheless the effects of cyber as a peril causing losses on policies remains and for some lines of business may never be eradicated. An example of this could be a credit risk portfolio offering coverage as part of defaults on loans. The loan default may be a result of a cyber attack on a firm resulting in the firm being unable to pay and then triggering the insurance policy. The direct cause of the loss is the loan default, but the indirect causation could be defined as a cyber. There are many more potential situations like this across many lines of business which ultimately require insurers to think more carefully about cyber/IT as a risk driver across their underwriting portfolios.

17. In terms of a CNI event, the potential for this to cause losses across the market on non-cyber products does exist. Perhaps in a similar way that was seen from COVID-19 the losses insurers face are likely due to areas of policy wordings that are open to interpretation or lack of awareness that the line of business could be exposed in such events. Again, the scale and

length of the CNI event will drastically affect the potential losses. Fundamentally the sector is only at risk if the losses caused (both in terms of claims and operational risks) from any CNI event put the solvency of the market under pressure. In such cases the regulators will need to decide if solvency rules or support should be provided to support the industry.

18. In any case insurers lack the appetite or capacity to offer the market coverage for a CNI event. It is likely that this type of event would be too big for the market to support both on an affirmative basis but more so on a non-affirmative basis. This does increase the financial and knock-on impacts of CNI events to the broader economy.

Life Insurers

19. Although not writing cyber insurance, life insurers are not immune from the evolving cyber risk environment.

20. Exposure for life insurers arises through three overarching groups of scenarios which may be expected to share similar characteristics:

    a. External risks – Cyber events occurring to national infrastructure which may both directly impact the living standards of customers, and could also affect the operations of industry, including the ability to serve customers

    b. Industry risks – Cyber events occurring to other companies in the financial services industry, such as outsourcers, which may impact a firm.

    c. Internal – Cyber events impacting a firm's own systems and processes, which impacts ability to manage policies and serve customers.

21. The most impactful events are likely to result from power events, coupled with weather events as discussed below.

External Risks

22. This group of scenarios includes cyber risk events occurring in the external environment, most likely caused by nation states looking to destabilise adversaries:

    a. Healthcare systems - Restricted access to medical care, through loss of access to either patient records or functioning of equipment.

    b. Payment systems - Limited payment systems make it difficult for a life insurer to make benefit payments, and therefore for policyholders to purchase living essentials.

    c. Communication systems - Instability of communication network disrupts market trading. Policies are difficult to value as well as to encash for customers.

    d. Power systems - These scenarios are likely to have an impact on all the above, plus the functioning of heating and refrigeration systems. If occurring at the same time as weather events there is the possibility of having a significant impact due to the compounding of the natural catastrophe event and the loss of CNI. An example of this is severe cold, coupled with CNI used for heating, coupled with power loss impacting the ability of the NHS to service those who fall unwell. This is a very unlikely combination of events but is possible.

23. Each of these scenarios is likely to have some impact on operations and mortality experience for a life insurer. Power systems are likely to have the most widespread impact, although it is likely that these systems will be manually brought back online within a few hours.

24. Where communication or payment systems are impacted, these are likely to require specialist expertise to repair. Availability of such expertise may be limited in scenarios where the impacts are widespread.

25. Although these scenarios may result in a number of economic, demographic and operational risks being realised together in a short period of time, the operations of a life insurer are likely to recover shortly after systems are restored.

Industry and Internal Risks

26. These groups of scenarios are caused by targeted attacks on the systems of individual firms or industries.

27. Systems outage scenarios are likely to be triggered by a Distributed Denial of Service (DDoS) or a ransomware attack rather than CNI driven events, but one form of CNI event is that they may also arise where a nation state targets the financial system of a country.

28. In the scenario where a ransomware attack has taken advantage of an unpatched vulnerability, multiple firms are likely to be impacted at the same time. Wannacry is an example where organisations not patching their systems in a timely way gave attackers time to develop the ransomware and successfully deploy it on a large scale in multiple companies over a short period of time.

29. In these scenarios, it may be difficult to secure the required external expertise due to the number of firms impacted at the same time. Larger firms are likely to have such expertise, but markets and policyholders could be disrupted for a period of time in this scenario.

Understanding the uncertainty in cyber outcomes

30. The IFoA Cyber Risk Working Party has also produced a paper – "Cyber Risk within Capital Models"[iii] – to help insurance firms with their considerations when it comes to setting capital for cyber risk exposures, whether through actively writing cyber risks, operational cyber risks, or both. This is relevant to the fourth point in the Call for Evidence regarding the government's approach to standards and regulations for cyber resilience and preparedness. The insurance industry has a key role to play, which will only increase with time, in our stance against the nation's cyber risks, and solvency adequacy is a vital component that must not be overlooked in resilience conversations.

31. As with most developing or ever-evolving risks on the threat landscape, concerns have already been raised about the adequacy of cyber quantification by key regulatory players over the years. This includes market feedback given by the PRA[iv] as well as cyber specific solvency capital deep dives by Lloyd's of London. However, progress on developing the sophistication behind the quantification of cyber risks has been slow and this directly has knock-on impacts onto solvency capital setting developments also. As the demand for cyber insurance increases as we look to the future, solvency calculations for this risk need to also develop proportionately. In many cases, capital calculations for cyber exposures held by (re)insurers are still relatively primitive.

32. There are many ways in which improvements could be made, at least initially, by adding depth to calculations, as is explained in the working party's paper. However, the government and regulators have a key role to also play as this is a relatively new risk that is ever evolving and data is scarce. There are no true sizeable events yet in the data that (re)insurers can use to help them validate their assumptions in pricing and for capital purposes. Unfortunately, as with a number of evolving risks, overconfidence bias becomes a key threat in such situations as (re)insurers may feel that they are adequately prepared when, in reality, they are yet to be tested (and their own resilience tests/capital allowances are inadequate); data can help with this key area of resilience building. The government may be able to assist through collaborations in allowing (anonymised) data-sharing, where possible, to allow insurers insights into this risk that the government may be privy to, amongst other best practice learnings as the cyber risk develops.

Referenced papers

[i] *Operational Cyber Risk*

https://www.actuaries.org.uk/learn-develop/attend-event/sessional-research-event-cyber-operational-risk-scenarios-insurance-companies

[ii] *Non-affirmative Cyber Risks/Cyber as a Peril*

https://www.actuaries.org.uk/documents/introduction-silent-cyber-assessment-framework

[iii] *Cyber Risk within Capital Models*

https://www.actuaries.org.uk/documents/cyber-risk-working-party-capital-models

[iv] *PRA view on cyber quantification*

https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2023/insurance-stress-test-2022-feedback.pdf?la=en&hash=A680452E3B0B5EA3EA2FC5E470EBEF3B66A58DD5